Amendments to the Claims

1. (Currently Amended) A method comprising:

generating a list of update keys on a key distribution center system based on a table of secret keys identifying the valid and invalid receivers of a plurality of receivers, the list of update keys allowing valid receivers to decrypt a valid content key using update keys obtained from the list of update keys;

generating a multiple nested list of decryption patterns based on the list of update keys;

encrypting each of the update keys using the corresponding secret key assigned to each of the valid receivers;

broadcasting the multiple nested list of decryption patterns to the plurality of receivers; and

recovering a content key from the list of update keys by recovering a set of update keys for each receiver from the multiple nested list of decryption patterns and using the set of update keys to decrypt the content key, wherein the valid receivers receive the recovered content key to facilitate decryption of content, and each of the invalid receivers ~~receives~~ to receive an intermediate key indicating to the key distribution center that an invalid receiver is to have the content blocked to facilitate blocking of the content.

2. (Previously Presented) The method of claim 1, wherein the generating of the list of update keys comprises generating one or more distinct intermediate keys and the content key.

3-4. (Canceled)

5. (Previously Presented) The method of claim 1, wherein the generating of the multiple nested list of decryption patterns comprises encrypting an entry of the list of update keys using a key that comprises a combination of a previous update key, a secret key for a receiver associated with the entry of the list of update keys, and an index indicating a location in the table of secret keys associated with each entry.

6. (Previously Presented) The method of claim 5, wherein an entry in the multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret key for the receiver associated with the entry of the list of update keys.

7. (Previously Presented) The method of claim 1, wherein the recovering of the set of update keys for each receiver from the multiple nested list of decryption patterns comprises parsing the multiple nested list of decryption patterns to locate an entry intended for a particular receiver based on detection of a predetermined test pattern included in an entry in the multiple nested list of decryption patterns.

8. (Previously Presented) The method of claim 1, further comprising broadcasting the content encrypted with the content key.

9. (Previously Presented) The method of claim 8, further comprising decrypting the content encrypted with the content key using a content key recovered from the multiple nested list of decryption patterns.

10-18. (Canceled)

19. (Currently Amended) A system comprising:

a key distribution center to

generate a list of update keys based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, the list of update keys allowing valid receivers of the plurality of receivers to decrypt a valid content key using update keys obtained from the list of update keys, generate a multiple nested list of decryption patterns based on the list of update keys, encrypt each of the update keys using the corresponding secret key assigned to each of the valid receivers, and

broadcast the multiple nested list of decryption patterns to the plurality of receivers; and

a content receiver to recover an appropriate set of update keys from the multiple nested list of decryption patterns so that the final key recovered in the set of update keys comprises a content key, wherein the valid receivers receive the recovered content key to facilitate decryption of content, and each of the invalid receivers ~~receives~~ to receive an intermediate key indicating to the key distribution center that an invalid receiver is to have the content blocked to facilitate blocking of the content.

20. (Previously Presented) The system of claim 19, wherein the key distribution center generates one or more distinct intermediate keys and the content key.

21-22. (Canceled)

23. (Previously Presented) The system of claim 19, wherein the key distribution center encrypts an entry of the list of update keys using a key that comprises a combination of a previous update key, a secret keys for a receiver associated with the entry of the list of update keys, and an index indicating a location in the table of secret keys associated with each entry to generate the multiple nested list of decryption patterns.

24. (Canceled)

25. (Previously Presented) The system of claim 19, wherein the receiver parses the multiple nested list of decryption patterns to locate an entry intended for a particular receiver based on detection of a predetermined test pattern included in an entry in the multiple nested list of decryption patterns.

26. (Previously Presented) The system of claim 19, further comprising a content provider to broadcast the content encrypted with the content key.

27. (Canceled)

28. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to:

generate a list of update keys on a key distribution center system based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, the list of update keys allowing valid receivers to decrypt a valid content key using update keys obtained from the list of update keys;

generate a multiple nested list of decryption patterns based on the list of update keys;

encrypting each of the update keys using the corresponding secret key assigned to each of the valid receivers;

broadcast the multiple nested list of decryption patterns to the plurality of receivers; and

recover a content key from the list of update keys by recovering an appropriate set of update keys for each receiver from the multiple nested list of decryption patterns and using the set of update keys to decrypt the content key, wherein the valid receivers receive the recovered content key to facilitate decryption of content, and each of the invalid receivers ~~receives~~ to receive an intermediate key indicating to the key distribution center that an invalid receiver is to have the content blocked to facilitate blocking of the content.

29. (Previously Presented) The machine-readable medium of claim 28, wherein the generating of the list of update keys comprises generating one or more distinct intermediate keys and the content key.

30-31. (Cancelled)

32. (Previously Presented) The machine-readable medium of claim 28, wherein the generating of the multiple nested list of decryption patterns comprises encrypting an entry of the list of update keys using a key that comprises a combination of a previous update key, a secret key for a receiver associated with the entry of the list of update keys, and an index indicating a location in the table of secret keys associated with each entry.

33. (Previously Presented) The machine-readable medium of claim 32, wherein an entry in the multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret key for the receiver associated with the entry of the list of update keys.

34. (Canceled)

35. (Previously Presented) The machine-readable medium of claim 28, further comprising broadcasting the content encrypted with the content key.

36. (Previously Presented) The machine-readable medium of claim 35, further comprising decrypting the content encrypted with the content key using a content key recovered from the multiple nested list of decryption patterns.

37-45. (Canceled)